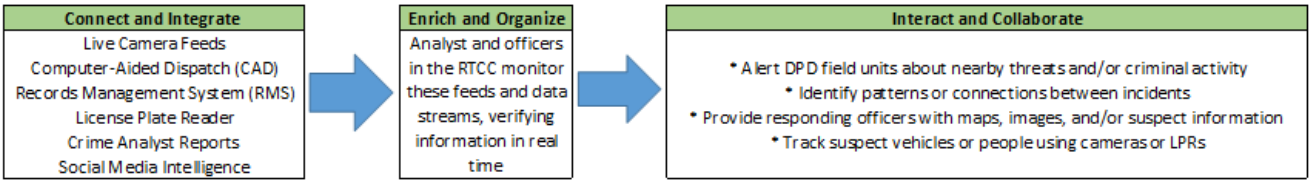
Real-Time Crime Center/Peregrine Town Hall Meetings

Date	Location	Attendance	Time
November 4, 2025	W.D. Hill	8	6pm-8pm
November 5, 2025	Weaver Street	8	6pm-8pm
November 6, 2025	Virtual	17	6pm-8pm
November 8, 2025	Lyon Park	8	12pm-2pm
November 12, 2025	Holton	19	6pm-8pm
November 13, 2025	Virtual	11	6pm-8pm
November 14, 2025	Virtual	7	6pm-8pm

Real Time Crime Center history

- A Real-Time Crime Center (RTCC) is a technology driven hub used to improve public safety and enhance emergency response. The proposed RTCC will use Peregrine Technology software to help solve crimes quicker by filtering through existing data within our system to compile information quickly. Peregrine Technologies integrates multiple data sources and tools into one centralized location.


Connect and Integrate
Live Camera Feeds
Computer-Aided Dispatch (CAD)
Records Management System (RMS)
License Plate Reader
Crime Analyst Reports
Social Media Intelligence
Enrich and Organize
Analyst and officers in the RTCC monitor these feeds and data streams, verifying information in real time
Interact and Collaborate
* Alert DPD field units about nearby threats and/or criminal activity
* Identify patterns or connections between incidents
* Provide responding officers with maps, images, and/or suspect information
* Track suspect vehicles or people using cameras or LPRs

Overall the RTCC is a mission control center for public safety; combining technology, data, and human analysis to help law enforcement work smarter and faster.

FAQs:

1. **High-level examples are nice; however, I am still unclear how Peregrine works?**

- Peregrine will utilize existing data from DPD systems, such as the 911 Computer-Aided Dispatch system and the Records Management System. Peregrine organizes and consolidates this information, which is then verified by analysts and/or officers before being shared with DPD field units. Peregrine does not collect or record any new information. Peregrine does not provide any sensors or cameras. The platform only uses data that already exists within DPD systems—it is not a surveillance platform. For example, for a different Peregrine customer, a young child with special needs was recently found standing in an intersection, and responding officers were unsure where to take her. Police records can be very siloed, and without Peregrine, officers would have likely taken the child to social services and waited for someone to report her missing. With Peregrine, officers were able to draw a digital radius on the map and quickly search

for calls related to a child matching her description. They located a relevant 911 call for a past incident, went to the address, and reunited the child with her family within an hour. The mother had not yet realized the child had crawled out of a window. Peregrine ensures that critical information is delivered to officers and investigators in real time, allowing for faster, more informed responses.

2. **What will Peregrine be doing for the community? What are their goals?**

- The goal is to provide officers with better-informed responses, solve complex cases more quickly, increase closure rates, allocate resources more effectively, and deliver information to the community at a much faster rate.

3. **Will Durham work with other agencies to share information?**

- Collaboration among agencies is only permitted when both agencies agree to it. Durham would have to opt in to enable this feature for sharing information. Any outside agency must formally request permission from DPD to access information within Peregrine. If DPD chooses to grant access, they must provide written authorization to Peregrine. There is no automatic or open sharing of information—Peregrine will follow the explicit instruction from Durham.

4. **It is stated in the Peregrine contract that groups with permission can gain access to the DPD data. What is the process for a non-DPD entity to gain access to Peregrine? Would DPD share when and with whom they allow access to their Peregrine system? Would they be able to view the information from their phones? Can they access the information outside of Durham? How long could they view the information for?**

- All data brought into Peregrine will remain within the platform. No DPD data will be shared without explicit written authorization from DPD. DPD employees will have varying levels of access to data as authorized by DPD leadership; Leadership will have full access and will share pertinent information with staff as needed. While DPD can choose to allow limited information sharing with neighboring departments, this is not the current intention. DPD retains full control over what information is shared, with whom and how long another agency may access it. Additionally, authorized users can access the information from any mobile device, allowing them to view the platform during patrol duty, for example.

5. **Has the department decided which agencies to engage in interconnects with, and how to respond to interconnect requests from others?**

- No, we have not decided, and we do not yet know if we will participate in data sharing. If we did, it would all be documented in writing and would need approval.

6. **What is clean data?**

- Clean data refers to information that is accurate, complete, consistent, and free of errors or duplicates. It is data that has been reviewed, corrected, and organized so it can be used confidently for analysis or decision-making. Clean data typically means: no typos or incorrect entries, no duplicate records, no missing important details, information is formatted consistently, outdated or irrelevant information is removed. For example, if you have multiple entries for the same person with different spellings of their name, or if a phone number is typed incorrectly, that would be considered dirty data. Cleaning it ensures everything matches, makes sense, and is reliable.

7. **While Peregrine has never had a data breech, what would be the protocol if they did?**

- Peregrine would be required to notify DPD immediately in the event of becoming aware of a breach. DPD would then release information about the breach to the public. Peregrine undergoes extensive security testing and employs strong safeguards to protect data, and they do not anticipate this ever occurring—as such an incident would jeopardize the company's entire reputation and operation.

8. **Would our information be more vulnerable (easier to get hacked)? What countermeasures does Peregrine have to protect our data (in simple terms)?**

- It would be no more susceptible than it is today. Peregrine maintains 24/7, year-round security monitoring to protect client data. They hold multiple certifications and use several layers of encryption to ensure information remains secure. A data breach would undermine the company's credibility, so data protection is their highest priority. This protection also applies to archived data. If the contract with DPD were to end, all data and records would be permanently deleted.

9. **What security features will be put in place to keep this information safe?**

- This cloud environment is built for local governments, and it has to meet certain standards which is determined by federal and state government. There's a rigorous set of standards we have to meet. Peregrine is not a data broker and has never sold or brought data. Peregrine will only and has only facilitated data sharing when its customers have explicitly requested it does so. These are part of the contractual terms we abide by.

10. **What happens if someone internal hacks Peregrine's system and gains access to our information?**

- DPD is proud of its accountability processes, even when they result in personnel separation. Compliance reports are routinely generated and made available for public review.

11. If Durham already has a good accountability process then why aren't we using more humans versus systems that clean data?

- Humans are not without flaws or errors, and the same is true for any technology. However, the advantage of this technology is its ability to process information and produce results much faster than a human can.

12. What is the process for accountability when there's an error in the data?

- The affected resident would be notified, and any error within the system would be corrected. A system is only as reliable as the information provided by its human operators.

13. What is predictive policing?

- Predictive policing uses historical crime data, trends, and patterns to anticipate potential criminal activity. Peregrine Technologies does not use predictive policing. They do not predict where crime is going to happen. They offer analytics to look at crime trends for resourcing decisions.

14. How do you differentiate safety flags from predictive policing?

- Predictive policing does not make absolute statements like "we believe this location will experience two robberies this weekend" or "we believe this person will harm their neighbor tomorrow." Instead, it identifies patterns and risk factors based on historical data to forecast future activity. Safety flags, for example, alert officers that an individual, such as Joe Smith, has previously responded aggressively when approached, allowing officers to be informed and take appropriate precautions, but safety flags do not make any forecast or predictions about future criminal activity.

15. What are social media warrants?

- They are COURT ORDERS that allow law enforcement agencies to legally access information from someone's social media accounts as part of an active criminal investigation. Peregrine Technologies does not gather information from any social media; it only integrates its customers' existing data sources. However, once an agency obtains a court order for a social media warrant and inputs it into their system, Peregrine can house that information from the agencies data.

16. What is Insight?

- A separate company specializing in license plate recognition technology. This would be a separate data source that would be purchased by DPD and integrated into Peregrine; if approved. LPR cameras can be fixed or mobile to capture license plates. Insight information would be used for violent crimes, missing persons, and amber alerts.

17. Are you working to access Insight as a provider?

- Yes, we are considering acquiring Insight as a provider. Insight operates differently from Flock. Insight does not sell or share its data; the information remains the property of the owner and is not released to the public. In contrast, Flock's information is publicly accessible.

18. Are there safeguards in place for the Insight software?

- As with all our data, officers must verify the license plate against the bulletin and then verify with the Division of Criminal Information (DCI).

19. Does DPD work with Flock products?

- DPD does not actively use any Flock products; however, a Memorandum of Understanding (MOU) is in place. DPD is aware that some communities and private businesses in Durham have Flock systems. If a crime occurs in a specific area and DPD knows that a community or business uses Flock, we may request that they share relevant footage to aid the investigation. The community or business retains the right to decline.

20. If we used files from Flock, would Flock have access to our Peregrine system?

- No, the data would flow in from Flock to Peregrine but not the other way around.

21. What are your thoughts on Peregrine CEO, Nick Noone being previously employed by Palantir?

- When situations or environments no longer align with your purpose, you have the right to move on. The values of Palantir differ significantly from those of Peregrine.

22. How are you getting information out so that all the citizens of Durham can share their input?

- We are hosting multiple (eight) meetings at various locations and times throughout the city to include as many citizens as possible. Additionally, the information has been made available on the DPD website. It can be found on this webpage: https://www.durhamnc.gov/5473/Real-Time-Crime-Center, which is the same approach we used with ShotSpotter. We are doing this so the public has access to the same information that we have.

23. Does this contract already exist? Was there an opportunity for community input beforehand?

- This contract does not yet exist. It was presented to the council during a work session as a proposed multi-year agreement with Peregrine. The council requested that we gather additional input from the community before moving forward. The contract must go through another city council work session and then be voted on. If approved, Peregrine engineers will spend several months in Durham reviewing and integrating existing data, visiting neighborhoods, participating in ride-alongs, and providing training for officers.

24. How are contracts with Technology Solutions brought forward for consideration?

- We follow a thorough vetting process to ensure all points are addressed. Once solutions are vetted and a cybersecurity review is completed, we confirm that appropriate insurance is in place. We work closely with the City Attorney's Office to ensure the contract language is correct and all requirements are met. Once all needs are addressed, the contract is submitted as an agenda item. Depending on the contract's dollar amount, it will be reviewed by either the City Council or the City Manager. The contract is then either approved or rejected. If signed by the City Manager, we work with the vendor to implement the agreement.

25. Even though the community has concerns with this technology, is the police department still going to move forward with this contract?

- We plan to move forward with the contract so that it can be placed on the Council's agenda.

26. What is the implementation timeline?

- If approved, the program would begin with a 90-day trial involving a small group of investigators and crime analysts. This phase would help determine how the program can be most efficiently integrated. After this trial, we would expand further within the program's implementation phase.

27. Does Peregrine sell the data that they have gathered?

- No, the data stored with Peregrine legally belongs to the Durham Police Department. The information can only be shared with DPD's written permission or as required by law. Peregrine is not a data broker and does not sell or buy data.

28. Will Peregrine be able to sell information with any partner organizations? Organizations such as ICE?

- No. The data is not Peregrine's to sell, nor is Peregrine a data broker that sells or buys data. The data belongs solely to the Durham Police Department. We will not provide data to ICE or any federal agency. We understand the concern given the current environment. Peregrine only releases data if explicitly instructed to do so in writing by DPD or required by law. None of the information DPD provides to Peregrine is of interest to ICE. We do not ask reporting parties or suspects about their immigration status, as it is irrelevant to investigating cases. It is important that our community hears this so they can trust us. Peregrine is not contracted with ICE.

29. What happens if ICE contacts Peregrine with a warrant?

- ICE would not have any greater access than they would if they subpoenaed DPD's Records Management System. They would need to make a very specific request and could not gain open or continuous access to the entire system. Arrest records are already

publicly available online and include names, addresses, dates, and similar information. We do not store legal status information in the data shared with Peregrine, so ICE would not find anything relevant there. Our U-Visa information, to which they already have access, contains more legal status information than anything sent to Peregrine. Peregrine is not aware of any federal agency being able to compel access to an entire account—it would be akin to forcing access to every record in the DPD Records Department. Agencies can compel specific pieces of information, but not full logins or ongoing access. Our attorneys carefully review any warrants and will file injunctions if a search is deemed unjust.

30. How would Peregrine be using and retaining data (like audit data)?

- Peregrine does not own any customer data. They require access to DPD data to provide their services, such as audit trails. The data is not removed from DPD's system; it is replicated into Peregrine for modeling and analysis. This analysis helps the department understand usage patterns, such as which divisions use Peregrine most, periods of low usage, and the most frequently searched items. Peregrine owns the insights, not the underlying data. Additionally, Peregrine adheres to DPD's current data retention policy.

31. What is the cost of the program?

- $515,000 over 3 years ($172.5k annually)

32. Are there other things we are getting in tandem with Real Time Crime Center (RTCC)?

- We would like to bring in additional resources with ready-to-use operations, but this is not included in the current budget cycle. We applied for a grant through the DOJ; however, this administration pulled all law enforcement grants, so we were unable to access that funding as planned. We have since written letters advocating with state senators to pursue earmarked funding. Additionally, we applied for a $2 million grant for the RTCC to help cover future expenses.

33. According to Peregrine's website and presentation, there is AI used in the platform. What data is being used to train the AI system, so it knows what we are looking for?

- All generative AI features are completely optional and can be turned off at any time. AI is helpful for processing documents that cannot be easily searched, such as handwritten notes, and can read them just like PDFs. It can also extract text from photos, de-duplicate data, and create case summaries from multiple documents, converting stacks of paperwork into concise bullet points. Each bullet point includes links to the original documents, allowing humans to verify all information. No department data will ever be used for AI training purposes without explicit permission.

34. How can we feel confident with the software engineers having data access? What is their vetting process?

- All Peregrine personnel assigned to DPD undergo a background check and fingerprint scan. Peregrine hires based on both skill and integrity. Additionally, DPD has the final approval on whether any Peregrine employee can work on the project. Every view and click within Peregrine is fully audited and permanently recorded.

35. Does Peregrine own the data?

- Peregrine only owns the insights created by the department using the data. They do not own any crime data.

36. Does Peregrine have their own data provider?

- Peregrine is hosted in AWS GovCloud. It is built to align with government data standards.

37. Once Peregrine system is in place, could commercial data brokers then purchase data under the veil of creating new and innovative ways to use the existing data?

- Absolutely not. The existing data will not and cannot be sold and we do not intend to entertain commercial data brokers.

38. What other agencies use Peregrine?

- Agencies in the region - locally and nationwide – utilize Peregrine, and they've had to go through the same process. Peregrine supports hundreds of public safety agencies across 26 states. Raleigh Police and Cary Police use Peregrine.

39. Were Peregrine competitors considered?

- Competitors were evaluated from a cost perspective, and Peregrine was determined to be the best option. Peregrine offers exceptional availability at a favorable cost. If approved, this contract would span three years, after which standard software agreements would be negotiated to ensure continuity.

40. Can you talk about the infrastructure that will be necessary?

- Peregrine requires no new infrastructure, such as a newly constructed building, for the City of Durham. No additional servers are needed beyond what Peregrine already uses. The platform operates using Amazon's cloud service, AWS, which we determined was the best fit for our objectives and goals as a company.

41. Is there a contractual guarantee that Peregrine won't start using facial recognition technology?

- Peregrine does not operate or deploy facial recognition technology. Peregrine only integrates its customers' existing data sources that its customers lawfully possess in accordance with local, state, and federal laws. Peregrine is required to notify clients of

any new technology it intends to deploy. If a new capability is introduced and the department (Durham Police) objects to its use, they have the option to terminate the contract.

42. Is there a penalty for cancelling the contract?

- There is no penalty for cancelling. At any time, the City can cancel the contract. On an annual basis, the City must decide if they want to allocate the money for it.

43. How do we ensure officers will be able to use the program to its full capacity?

- DPD will train officers to use the program. DPD will also utilize audits to follow what the system is used for by each officer. It will be no different than people relying on ChatGPT – we have to be able to audit their actions.

44. Are the taxpayers footing the bill? Can we modify ShotSpotter so that the taxpayers do not have to pay for this?

- ShotSpotter helped us respond to gunshots more quickly, but there was no data indicating that it improved overall safety or prevented crimes from occurring. While there was some crime displacement, there was no measurable reduction in overall crime. Our goal with this initiative is to consolidate all existing information into a single system, making it faster to access and analyze. This approach would save both time and taxpayer dollars compared to manual processes.

45. Will the community have access? Will we be able to see perpetrators?

- The public will not have access to personnel records, but we do have public forums where they can view arrest records.

46. If this doesn't pass, what can the community do to help DPD in the future?

- Involvement. If we have a crime, it helps when people speak out to what they know/have seen. Someone always knows something and it would help our case closure rate for people to step forward.

47. Will public defenders and the DA's office be able to access the Peregrine information?

- The DA's office will have access to the case files, but not the entire Peregrine system. Peregrine makes it easier to ensure all data needed for discovery is included. All companies will only have access with written permission from DPD.

48. Would the intel officer jobs be less of a necessity with this new system? Could you just hire someone or multiple people to do this manually instead of using Peregrine?

- No, employees will not lose their jobs to Peregrine. Staff are required to verify all information compiled by the system, especially when AI is used. We will not rely solely on software without human review. Currently, several employees—such as those in the

Records Department—manually review information, a time-consuming process that spans 5–10 different departments. Peregrine will reduce this manual workload, allowing auditors to focus their expertise on directly assisting cases more efficiently.

49. Could DPD just use the salaries from all the open department slots to put towards the Peregrine program instead of the tax dollars?

- That funding is allocated for LAP salaries and covers supplemental patrol to compensate for staffing shortages. However, the amount is expected to decrease as our academy classes grow—currently 32 recruits, with the upcoming class projected at 50.

50. Will DPD be collecting more data to add to Peregrine?

- Yes, the same data that would normally be added to our manual systems will be added to Peregrine. Photos, videos, and tips can still be collected and uploaded through out usual channels.

51. Would the RTCC be a new, separate building?

- No, it will be within the Police Department.